

IN THE SPECIFICATION:

On page 4, amend the paragraph beginning with "Method A Decryption" as follows:

The expression $[c_1, c_2, c_3, c_4, c_5, \dots, c_n, \dots]$ represents ciphertext (encrypted message).

- i. Use a key to build a state generator, and a sequence of inverse permutations. (Subsection J.)
- ii. Apply the sequence of inverse permutations to the ciphertext so that the order is permuted: $[c_{i1}, c_{i2}, c_{i3}, c_{i4}, c_{i5}, \dots, c_{in}, \dots]$. (Subsections B and C.)
- iii. Use the state generator to create a sequence of states: $[s_{i1}, s_{i2}, s_{i3}, s_{i4}, s_{i5}, \dots, s_{in}, \dots]$ ~~$[s_1, s_2, s_3, s_4, s_5, \dots, s_n, \dots]$~~ .
- iv. Use state s_{i1} ~~$[s_1]$~~ to decrypt ciphertext element c_{i1} . Use state s_{i2} ~~$[s_2]$~~ to decrypt ciphertext element c_{i2} . Use state s_{i3} ~~$[s_3]$~~ to decrypt ciphertext element c_{i3} , and continue on, all the way up to use state s_{in} ~~$[s_n]$~~ to decrypt ciphertext element c_{in} . And so on.

On page 5, amend the paragraph beginning with "Comments on Method A" as follows:

~~In method A, step iii may precede ii or step ii may precede iii, or they can be executed simultaneously.~~ There is an alternative way of decrypting in method A.

- ii. Use the state generator to create a sequence of states: $[s_1, s_2, s_3, s_4, s_5, \dots, s_n, \dots]$. (Subsections D, E, F, G, H, and I.)
- iii. Use state s_1 to decrypt ciphertext element c_1 . Use state s_2 to decrypt ciphertext element c_2 . Use state s_3 to decrypt ciphertext

element c_3 , and continue on, all the way up to using state s_n to decrypt ciphertext element c_n . And so on.

- iv. Apply the sequence of inverse permutations to the scrambled plaintext $[c_{i1}, c_{i2}, c_{i3}, c_{i4}, c_{i5}, \dots, c_{in}, \dots]$ so that the order is permuted back to the original plaintext message, $[d_1, d_2, d_3, \dots, d_n, \dots]$.
(Subsections B and C.)